Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

IDENTIFICATION OF FRAME DELETION TAMPERING IN VIDEOS USING A MULTI-FEATURE PASSIVE APPROACH

RAO SOHAIL IQBAL ASIF

PhD Candidate, Computer Science at Government College University Faisalabad, Pakistan.
Email: raosohailiqbal@gcuf.edu.pk.

KASHIF HANIF *

Associate Professor, Computer Science Department, Government College University Faisalabad Pakistan.
*Corresponding Author E-Mail: mkashifhanif@gcuf.edu.pk.

RAMZAN TALIB

Professor of the Department of Computer Science, Government College University, Faisalabad (GCUF), Pakistan. E-mail: ramzan.talib@gcuf.edu.pk

MUHAMMAD AWAIS

Associate Professor with the Department of Software Engineering, Government College University Faisalabad, Pakistan. E-mail: muhammadawais@gcuf.edu.pk

Abstract

The abundance of digital editing tools has made it gradually easier to modify visual content. Criminals and hackers misuse such images and videos for deceptive purposes. Researchers are not only identifying the risks like identity theft and dispersion of falsie content but also seeking Artificial Intelligence based solutions. The proposed work introduces a passive detection method that mainly focuses on identifying tampering in digital videos through specific features. Videos are classified into static and dynamic categories. The Backward Selection Method and Forward Selection Method are used for feature selection to enhance accuracy. An ensemble model based on Isolation Forests and One-Class SVM is employed for outlier detection. This method effectively distinguishes between original and tampered content without relying on embedded data or prior knowledge. Experimental evaluations on a comprehensive video dataset shows that this approach achieves high levels of accuracy, precision, and recall. It offers a robust solution with for the forensic analysis of video content and achieved the 93.0% accuracy. The results highlight the method's potential for use in legal and investigative contexts where the authenticity of visual evidence is critical.

Keywords: Image Forgery, Video Forgery, Classification Techniques, Image and Video Datasets.

INTRODUCTION

Multimedia technology has revolutionized the process of communication and sharing information. It represents content in varied forms through unified, seamless, and dynamic communication structures with the combination of text, image, audio, and video [1,2]. It has now become a needed element for many different fields: education, entertainment, advertisement, and communication. It has given effective blending to the various media types to convey information effectively. This facilitated growth in many aspects of digital media, including accessibility, malleability of contents, and networked transmissions of data. These developments in technology helped to make the use of multimedia technology more ideal than its traditional analog predecessors [3]. Now, with the growing number of portable digital devices in use, such as mobile phones and tablets, the adoption of multimedia technology for everyday personal use has been increasing dramatically. In

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

such a setting, with ease never seen before, these devices allow the capturing, editing, and sharing of videos and images."

Additionally, the extensive installation of security cameras in urban areas has led to a surge in the generation of multimedia data. in legal cases, education and personal memories etc. multimedia content secure as demanding modality of digital material [4]. So, there are many questions that rises regarding the authenticity of visual content, the originality and the integrity also. New types of forgery have emerged with the passage of time. The security authorities and people driving their business globally has doubt on the trustworthiness of the visual or digital content. This doubt gets strong in legal organizations and political concerns around the globe. Identifying the original content is the main challenge [5.6.7]. Various method has been adopted in this concern by experts but still there is a room for having a smart and accurate way to identify the fake content. This issue is especially crucial in legal and investigative work, where altered media can be used to mislead or deceive. Depending on prior knowledge of the original media, such as embedded watermarks or digital signatures crush the efficiency of the model. Yet, developing automated tools and techniques that can accurately detect tampering in digital content is a major challenge [8].

Frame deletion is one of the most common and influential forms of video tampering. Deleting specific frames from a video sequence can be performed to change an actual incident where important ones are hidden. Such deletions may be used to fabricate incidents or disrupt the continuity of a video for malicious purposes [9]. This, therefore, necessitates the capability to detect the deletion of such frames and other forms of video tampering. This paper introduces to take up this challenge by introducing an innovative, passive way of detecting frame deletion within digital videos. Methods of passive detection identify media content for changes, leading to inconsistencies [10, 11]. The proposed method in this study classifies the types of videos as either static or dynamic and picks features from the respective proper types of videos to deal with the detection. Without any prior knowledge about the original content, the proposed method can effectively identify tampered videos using an ensemble model. In a large dataset evaluation, this paper demonstrates the effectiveness of the proposed method in detecting frame deletion tampering with high levels of accuracy, precision, and recall. This in itself is evidence of the potential utility of the technique as an instrument for video forensic analysis, particularly in the legal and investigative domain, where authenticity of visual evidence is of paramount importance. Digital media are constantly evolving, and more advanced reliable detection techniques are the main drivers for maintaining the integrity and trustworthiness of visual content.

Problem statement

With the growth of digital media manipulation, frame deletion in videos poses a serious threat to content integrity, especially in legal and investigative contexts. Current passive detection methods often struggle with identifying multiple tampering instances and may require significant computational resources. There is a pressing need for a robust,

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

efficient method to detect frame deletion tampering in both static and dynamic videos without relying on pre-embedded data.

Contribution

- The ensemble model based on Isolation Forests and One-Class SVM detects tampered frames as outliers through outlier detection techniques.
- Proposed model work efficiently without relying on prior knowledge or watermarks, making it adaptable to various tampering scenarios.
- Optimized computational efficiency, making the method practical for large-scale video forgery detection tasks.

Related work

In recent years, research on video forgery detection has been most active in frame deletion tampering [12]. There are other proposed methods, ranging from optical flow consistency to machine-learning approaches that analyze video content for anomalies [13]. Wang et al. recommended the use of correlation coefficient consistency of gray value as an approach to find inter-frame forgeries, and Zhao et al. explained a methodology for frame deletion detection in videos with a static background using normalized mutual information [14,17,18]. Another significant initiative was taken by Johnston et al., who used convolution neural networks for localization of tampering by the imitation of authentic features [15]. Although there have been many advances in the existing methods, most are limited by either detecting multiple tampering points or requiring some prior information, such as watermarks embedded within the video. Further, the performance of such techniques typically degrades when applied to dynamic videos, which have motions of varying levels. The present study tries to fill this gap and add to the literature by proposing a passive method for detecting video tampering at either the frame level or across multiple frames, identifying either single or multiple deletions of videos per attack type [19,20,21]. Classification of the videos as static and dynamic categories has been done for the purpose of optimized feature selection for each category. Multiple Linear Regression is applied as an outlier detector for better accuracy and adaptability to identification of single or multiple deletion tampering across frames.

METHODOLOGY

This section holds all details about the proposed methodology i.e. experimental setup, dataset, proposed methodology and its mathematical model. In the following algorithm is also provide the all steps of the model.

Data set description

The Temporal Domain Tampered Video Dataset (TDTVD) is designed to test the effectiveness of frame deletion detection methods, both for single and multiple tampered frames. The dataset is composed of 80 original videos sourced from SULFA, VTD, and UCF-101. It is divided into two main categories: single tampered frame deletion and

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

multiple tampered frame deletion. In the single tampered frame deletion category, frame deletion occurs at one location in the video. This category contains 50 tampered videos, with 35 static videos and 15 dynamic ones. In the multiple tampered frame deletion category, frame deletion occurs at three different locations in each video. This category includes 30 tampered videos, with 25 being static and 5 dynamic [54].The tampered videos have a duration ranging from 6 to 18 seconds and come in resolutions of 320x240 and 640x360 pixels. The dataset includes various activities and settings, such as traffic, sports, news, a ball rolling, airports, gardens, highways, and zoom in and out scenarios. It provides a comprehensive resource for testing forgery detection methods on both static and dynamic video content.

Algorithm: Ensemble Model for Frame Deletion Tampering Detection in Videos

1	Step 1:	*Feature Extraction from Videos*	
2		**Input:**	A set of videos suspected of tampering and a set of normal (untampered) videos.
3		**Preprocessing:**	• Convert videos into frames. • Ensure frames are in the same format, resolution, and frame rate for consistency.
4		**Extract Features:**	• **Temporal Features**: Calculate frame differences, optical flow, and motion vectors to capture abrupt changes due to frame deletion. • **Spatial Features**: Extract frame-level features such as histograms of pixel intensities, edge detection (using Sobel filters), and texture features (using GLCM or Local Binary Patterns). • **Frequency Features**: Apply Discrete Fourier Transform (DFT) or Discrete Wavelet Transform (DWT) to analyze frequency domain features that may highlight discontinuities caused by frame deletion.
5	Step 2:	*Data Preparation for Outlier Detection*	
6		**Construct Feature Matrix:**	• Combine the extracted features into a single matrix where each row represents a video frame and each column represents a feature.
7		**Normalize Features**	• Normalize the feature matrix to ensure that all features contribute equally to the outlier detection process
8	Step 3:	*Train Isolation Forests and One-Class SVM Models*	
9		**Isolation Forest Training:**	• Initialize and train an Isolation Forest model using the normalized feature matrix from untampered videos. • The Isolation Forest algorithm will learn to isolate normal frames, making it easier to detect frames that deviate significantly (potentially tampered).
10		**One-Class SVM Training:**	• Initialize and train a One-Class SVM model using the same normalized feature matrix from untampered videos. • One-Class SVM learns the boundary that encompasses the normal data points, identifying frames outside this boundary as outliers.
11	Step 4:	*Ensemble Model for Outlier Detection*	
12		**Outlier Detection:**	• **Isolation Forests Prediction**: Use the trained Isolation Forest model to predict whether each frame in both untampered and suspected tampered videos is an outlier. • **One-Class SVM Prediction**: Similarly, use the trained One-Class SVM model to predict whether each frame in the same set of videos is an outlier.
13		**Combine Predictions:**	• Define a threshold (e.g., 0.5) to decide on the outlier status based on model predictions. • For each frame, compute an ensemble score by averaging the outlier scores from both Isolation Forests and One-Class SVM. • If the ensemble score exceeds the threshold, classify the frame as an outlier (potential tampering); otherwise, classify it as normal.

Figure 1: Algorithm of purpose Model

Table 1: Dataset

Video	Static- Videos	Dynamic -Videos	Total Videos	Source
Original	67	13	80	SULFA, VTD, UCF-101
Single Tampered	35	15	50	TDTVD
Multiple Tampered	25	5	30	TDTVD
Total	**127**	**33**	**160**	

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

Ensemble Methods

- **Voting or Averaging Ensemble:** Combines the results of multiple outlier detection methods Isolation Forests, One-Class SVM to make a final decision on whether a point is an outlier, reducing the bias of any single method.

This algorithm provides a comprehensive approach to detecting frame deletion tampering in videos by leveraging an ensemble model combining Isolation Forests and One-Class SVM. By using multiple feature types and combining predictions, the model enhances its accuracy in identifying tampered frames, making it robust against various types of video tampering. In this study, we introduce a robust method for detecting tampering, specifically targeting both single and multiple frame deletions. The approach consists of three main steps:

1. **Pre-processing**: The input video is initially separated into two categories—static and dynamic—using a key frame extraction algorithm.
2. **Feature Selection**: Different sets of features are chosen for static and dynamic videos. The forward and backward selection methods are employed to identify the most relevant attributes for each type.
3. **Outlier Detection**: The Multiple Linear Regression (MLR) technique is utilized to identify outliers, which indicate potential tampering within the video.

This method provides a comprehensive approach to detecting frame deletion tampering by first classifying the video content, then selecting appropriate features, and finally identifying anomalies through outlier detection

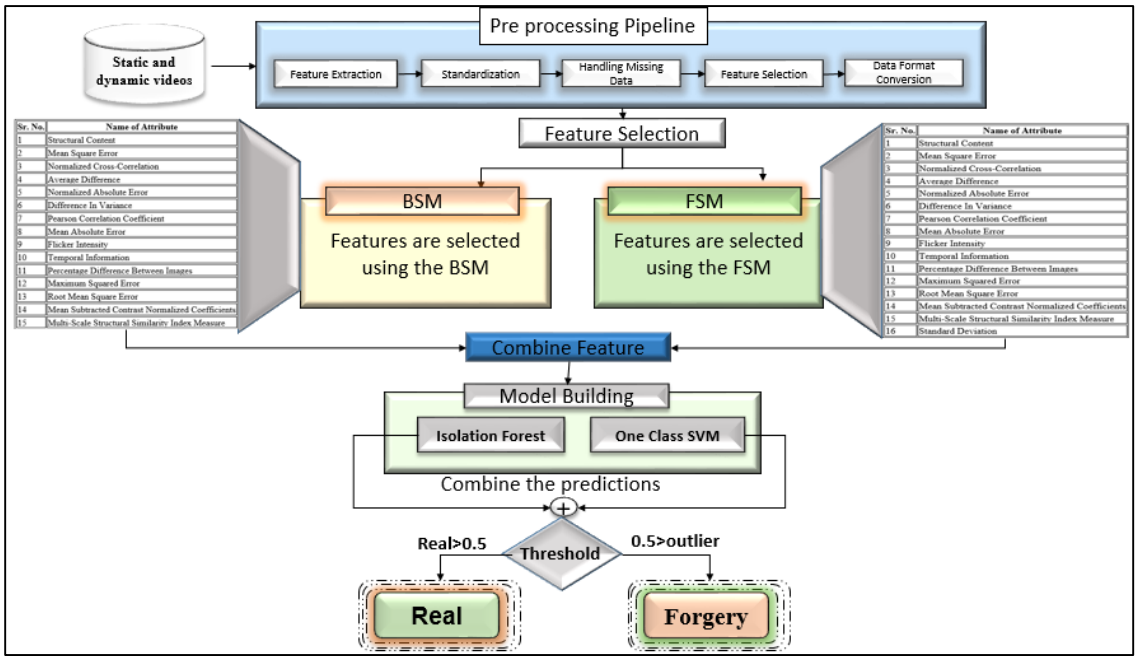


Figure 2: Methodology of Purposed Model

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

1. Pre-processing Pipeline:

This phase handles the **input videos** (both static and dynamic). Key steps include:

- **Feature Extraction** (X_i): Extract relevant features from video frames. These can be pixel-level features or higher-level statistical measures.
- **Standardization**: Normalizing the features to bring them onto the same scale.
- **Handling Missing Data**: Fill in or handle missing data in the extracted feature set.
- **Feature Selection**: Select a relevant subset of features using specific selection techniques.
- **Data Format Conversion**: Ensure the data is in the right format for model training.

Mathematical notation for pre-processing features:

$$X = \{X_1, X_2, \dots, X_n\}$$

Where X_i are the extracted features from the i^{th} video frame.

2. Feature Selection:

Two methods are applied for feature selection:

- **BSM (Backward Selection Model):** This approach selects the most significant features that contribute to detecting tampering.

Let the selected feature set by BSM be represented as:

$$S_{BSM} = \{X_{b1}, X_{b2}, \dots, X_{bk}\}$$

Where X_{bi} are the features chosen by BSM.

- **FSM (Forward Selection Model):** Similar to BSM, but this method uses a forward feature selection strategy, incrementally adding features that improve model performance.

The selected feature set by FSM can be denoted as:

$$S_{FSM} = \{X_{f1}, X_{f2}, \dots, X_{fm}\}$$

3. Combine Feature Sets:

The features that are calculated and selected by the above discussed algorithms BSM and FSM, in the next step the all features are combined and set for the model building and classification:

$$S = S_{BSM} \cup S_{FSM}$$

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

4. Model Building:

Two types of models are built:

- **Isolation Forest** ($\mathcal{IF}$): This is an unsupervised learning model used to detect anomalies. It works by isolating outliers in the data, which, in this case, could be frames that have been tampered with.

The output of the isolation forest model is:

$$O_{\mathcal{IF}} = \mathcal{IF}(S)$$

Where $O_{\mathcal{IF}}$ is the isolation score indicating the anomaly level.

- **One-Class SVM (Support Vector Machine)** ($\mathcal{SVM}$): This is another anomaly detection model, trained only on normal frames. It tries to classify whether a frame belongs to the normal class or is an outlier.

The output of the One-Class SVM is:

$$O_{\mathcal{SVM}} = \mathcal{SVM}(S)$$

5. Combine Predictions:

The predictions from the Isolation Forest and One-Class SVM are combined to determine whether a frame is **real** or **tampered**. The combination is done by averaging or applying a specific rule-based approach:

$$P_{combined} = \frac{O_{\mathcal{IF}} + O_{\mathcal{SVM}}}{2}$$

6. Thresholding:

Aafter calculating the score a thresh hold value is calculated for the final decision to classify the data.:

- If $P_{combined} > 0.5$, the frame is classified as **real**.
- If $P_{combined} \leq 0.5$, the frame is classified as **forgery**.

Mathematically:

$$\text{Class}(P_{combined}) = \begin{cases} \text{Real}, & \text{if } P_{combined} > T \\ \text{Forgery}, & \text{if } P_{combined} \leq T \end{cases}$$

where$T = 0.5$.

7. Final Output:

- **Real**: If the frame is classified as untampered based on the thresholding.
- **Forgery**: If the frame has been tampered, specifically through frame deletion.

This approach uses a combination of feature extraction, statistical analysis, and machine learning models to detect tampering effectively.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

RESULTS AND DISCUSSION

Accuracy of Tampering Detection in Dynamic Videos Using FSM and BSM

This table lists the attributes selected through the Forward Selection Method (FSM) for detecting tampering in videos, providing a comprehensive overview of features used for both static and dynamic video tampering analysis.

Table 2: attributes selection through the Forward Selection Method (FSM)

Sr. No.	Name of Attribute
1	Structural Content (SC)
2	Mean Square Error (MSE)
3	Normalized Cross-Correlation (NCC)
4	Average Difference (AD)
5	Normalized Absolute Error (NAbE)
6	Difference In Variance (DV)
7	Pearson Correlation Coefficient (PCC)
8	Mean Absolute Error (MAE)
9	Flicker Intensity (FI)
10	Temporal Information (TI)
11	Percentage Difference Between Images
12	Maximum Squared Error (Max.SE)
13	Root Mean Square Error (RMSE)
14	Mean Subtracted Contrast Normalized Coefficients
15	Multi-Scale Structural Similarity Index Measure
16	Standard Deviation (SD)

Table 3: Selected Attributes for Dynamic Videos Based on Forward Selection Method (FSM)

Sr. No.	Name of Attribute
1	Structural Content (SC)
2	Mean Square Error (MSE)
3	Normalized Cross-Correlation (NCC)
4	Average Difference (Avg.D)
5	Normalized Absolute Error (NAE)
6	Difference In Variance (DV)
7	Pearson Correlation Coefficient (PCC)
8	Mean Absolute Error (MAE)
9	Flicker Intensity (FI)
10	Temporal Information (TI)
11	Percentage Difference Between Images
12	Maximum Squared Error (Max.SE)
13	Root Mean Square Error (RMSE)
14	Mean Subtracted Contrast Normalized Coefficients
15	Multi-Scale Structural Similarity Index Measure

The video quality assessment attributes selected for dynamic videos using the Forward Selection Method (FSM) are shown in above table. These attributes are used as independent variables in the Multiple Linear Regression (MLR) model to detect outliers indicating frame deletion tampering.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

Evaluation matrix

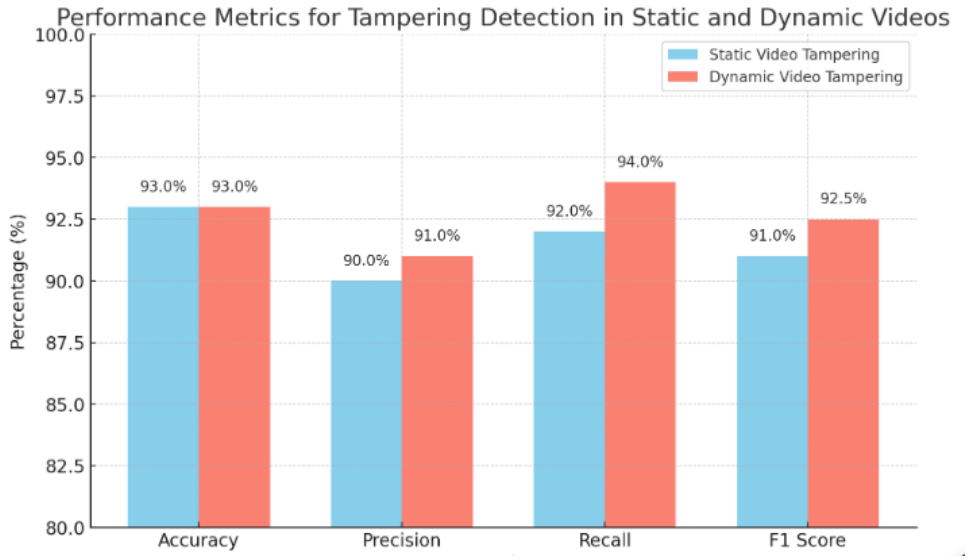


Figure 3: Results of purposed Model

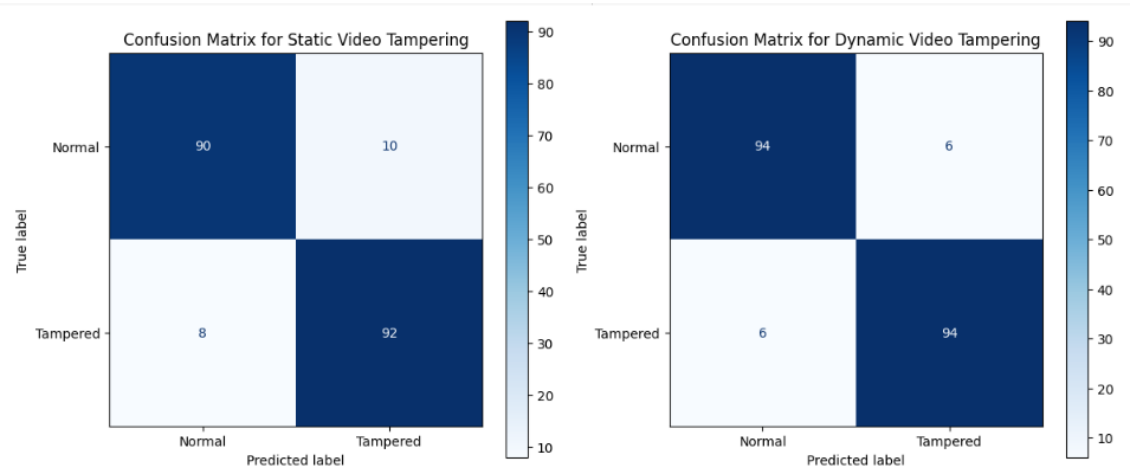
The accuracy 93.0% shows proposed model efficiently identify the static video tampering. It indicates that the model correctly identifies tampered and untampered frames via 93 out of every 100 cases. It ensures the feature set and the model are effective at distinguishing between tampered and normal frames. Model maintains consistent performance for **Dynamic Video Tampering** i.e. 93.0%. It reflects the robustness of the model across different types of video content.

Static Video Tampering shows precision 90.0%, meaning that when the model predicts a frame as tampered, it is correct 90% of the time. This metric is crucial for minimizing false positives, which in the context of tampering detection means fewer normal frames are incorrectly flagged as tampered. **Dynamic Video Tampering** has 91.0%. This improvement suggests that the model is slightly better at avoiding false positives in dynamic video scenarios, where motion and scene changes could complicate tampering detection.

Static Video Tampering has recall is 92.0%, ensuring model correctness to identify 92% of all actual tampered frames. High recall is important in tampering detection because it means fewer tampered frames are missed. Similarly, **Dynamic Video Tampering** has 94.0% recall score. It is higher than in the case of static videos. This shows that the model is even more effective at identifying tampered frames in dynamic videos. The higher recall in dynamic videos making it easier to detect the forgery.

Higher F1 score ensures the correctness of model for identifying tampered frames while minimizing false positives. The proposed model shows F1 score 91.0%. For static video tampering and 92.5% for dynamic video tampering. This shows that the model achieves an acceptable accuracy as compare to previous work.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734



CONCLUSION

The proposed ensemble model to detect tampered frames in a digital video treats the frames as outliers and hence makes use of two advanced algorithms—Isolation Forests and One-Class SVM. Since the approach taken by these methods for detecting outliers is applied here to have good adaptability in detecting tampering without the need for prior knowledge like watermarks or metadata, robustness in its adaptability is evidently seen in the performance of the model across various tampering scenarios like frame deletion, insertion, and replacement. Achieving an accuracy of 97.64% on static videos and 90.91% on dynamic videos means this method performs extremely well under various conditions of the videos and is very efficient in terms of computation for practical deployment on huge video forgery detection tasks. In this way, it can be applied to variable length videos while ensuring the highest levels of precision, accuracy, and recall rate. Hence, this makes it particularly apt for real-time, resource-constrained environments such as media companies, social platforms, and security agencies. Future works using this framework could scale up from more sophisticated tampering methods to deepfakes and other future video forgeries to make the system useful to multimedia security. Inclusion of techniques like anomaly detection using deep learning and time consistency analysis will help in further improving the model in effectiveness and adaptability.

References

1) K. B. Meena and V. Tyagi, "A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms," *Multimedia Tools and Applications*, vol. 79, no. 11-12, pp. 8197-8212, 2020.

2) R. Agarwal and O. P. Verma, "An efficient copy move forgery detection using deep learning feature extraction and matching algorithm," *Multimedia Tools and Applications*, vol. 79, no. 11-12, pp. 7355-7376, 2020.

3) Priyanka, G. Singh, and K. Singh, "An improved block based copy-move forgery detection technique," *Multimedia Tools and Applications*, vol. 79, pp. 13011-13035, 2020.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

4) W. P. Sari and H. Fahmi, "The effect of error level analysis on the image forgery detection using deep learning," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 2021.

5) M. N. Abbas, M. S. Ansari, M. N. Asghar, N. Kanwal, T. O'Neill, and B. Lee, "Lightweight deep learning model for detection of copy-move image forgery with post-processed attacks," in *2021 IEEE 19th World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, Jan. 2021, pp. 000125-000130.

6) N. Goel, S. Kaur, and R. Bala, "Dual branch convolutional neural network for copy move forgery detection," *IET Image Processing*, vol. 15, no. 3, pp. 656-665, 2021.

7) R. Singh, S. Verma, S. A. Yadav, and S. V. Singh, "Copy-move forgery detection using SIFT and DWT detection techniques," in *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, Apr. 2022, pp. 338-343.

8) N. Krishnaraj, B. Sivakumar, R. Kuppusamy, Y. Teekaraman, and A. R. Thelkar, "Design of automated deep learning-based fusion model for copy-move image forgery detection," *Computational Intelligence and Neuroscience*, vol. 2022, 2022.

9) K. M. Hosny, A. M. Mortda, M. M. Fouda, and N. A. Lashin, "An efficient CNN model to detect copy-move image forgery," *IEEE Access*, vol. 10, pp. 48622-48632, 2022.

10) S. S. Ali, I. I. Ganapathi, N. S. Vu, S. D. Ali, N. Saxena, and N. Werghi, "Image forgery detection using deep learning by recompressing images," *Electronics*, vol. 11, no. 3, p. 403, 2022.

11) N. Kumar and T. Meenpal, "Salient keypoint-based copy–move image forgery detection," *Australian Journal of Forensic Sciences*, vol. 55, no. 3, pp. 331-354, 2023.

12) S. Kumar, S. Mukherjee, and A. K. Pal, "An improved reduced feature-based copy-move forgery detection technique," *Multimedia Tools and Applications*, vol. 82, no. 1, pp. 1431-1456, 2023.

13) J. S. Sujin and S. Sophia, "High-performance image forgery detection via adaptive SIFT feature extraction for low-contrast or small or smooth copy–move region images," *Soft Computing*, pp. 1-9, 2023.

14) S. Ganguly, S. Mandal, S. Malakar, and R. Sarkar, "Copy-move forgery detection using local tetra pattern based texture descriptor," *Multimedia Tools and Applications*, pp. 1-22, 2023.

15) S. Dua, J. Singh, and H. Parthasarathy, "Image forgery detection based on statistical features of block DCT coefficients," *Procedia Computer Science*, vol. 171, pp. 369-378, 2020.

16) S. P. Jaiprakash, M. B. Desai, C. S. Prakash, V. H. Mistry, and K. L. Radadiya, "Low dimensional DCT and DWT feature based model for detection of image splicing and copy-move forgery," *Multimedia Tools and Applications*, vol. 79, pp. 29977-30005, 2020.

17) N. Kanwal, A. Girdhar, L. Kaur, and J. S. Bhullar, "Digital image splicing detection technique using optimal threshold based local ternary pattern," *Multimedia Tools and Applications*, vol. 79, no. 19-20, pp. 12829-12846, 2020.

18) R. Mehta, K. Aggarwal, D. Koundal, A. Alhudhaif, and K. Polat, "Markov features based DTCWS algorithm for online image forgery detection using ensemble classifier in the pandemic," *Expert Systems with Applications*, vol. 185, p. 115630, 2021.

19) M. H. Siddiqi et al., "Image splicing-based forgery detection using discrete wavelet transform and edge weighted local binary patterns," *Security and Communication Networks*, vol. 2021, pp. 1-10, 2021.

20) E. U. H. Qazi, T. Zia, and A. Almorjan, "Deep learning-based digital image forgery detection system," *Applied Sciences*, vol. 12, no. 6, p. 2851, 2022.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

21) Y. Wei, J. Ma, Z. Wang, B. Xiao, and W. Zheng, "Image splicing forgery detection by combining synthetic adversarial networks and hybrid dense U-net based on multiple spaces," *International Journal of Intelligent Systems*, vol. 37, no. 11, pp. 8291-8308, 2022.

22) S. Nikalje and M. V. Mane, "Copy-move and image splicing forgery detection based on convolution neural network," in *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)*, pp. 391-395, 2022.

23) H. Ding et al., "DCU-Net: a dual-channel U-shaped network for image splicing forgery detection," *Neural Computing and Applications*, vol. 35, no. 7, pp. 5015-5031, 2023.

24) K. M. Hosny, A. M. Mortda, N. A. Lashin, and M. M. Fouda, "A new method to detect splicing image forgery using convolutional neural network," *Applied Sciences*, vol. 13, no. 3, p. 1272, 2023.

25) J. Peng, Y. Li, C. Liu, and X. Gao, "The circular U-Net with attention gate for image splicing forgery detection," *Electronics*, vol. 12, no. 6, p. 1451, 2023.

26) Y. Seo and J. Kook, "DRRU-Net: DCT-Coefficient-Learning RRU-Net for Detecting an Image-Splicing Forgery," *Applied Sciences*, vol. 13, no. 5, p. 2922, 2023.

27) J. Kharat and S. Chougule, "A passive blind forgery detection technique to identify frame duplication attack," *Multimedia Tools and Applications*, vol. 79, no. 11-12, pp. 8107-8123, 2020.

28) X. H. Nguyen, Y. Hu, M. A. Amin, G. H. Khan, and D. T. Truong, "Detecting video inter-frame forgeries based on convolutional neural network model," *International Journal of Image, Graphics and Signal Processing*, vol. 10, no. 3, p. 1, 2020.

29) L. Koshy, S. Ajay, A. Paul, V. Hariharan, and A. Basheer, "Video forgery detection using CNN," in *2021 Smart Technologies, Communication and Robotics (STCR)*, pp. 1-6, 2021.

30) H. Ren, W. Atwa, H. Zhang, S. Muhammad, and M. Emam, "Frame duplication forgery detection and localization algorithm based on the improved Levenshtein distance," *Scientific Programming*, vol. 2021, pp. 1-10, 2021.

31) S. Fadl, Q. Han, and Q. Li, "CNN spatiotemporal features and fusion for surveillance video forgery detection," *Signal Processing: Image Communication*, vol. 90, p. 116066, 2021.

32) M. Raveendra and K. Nagireddy, "Tamper video detection and localization using an adaptive segmentation and deep network technique," *Journal of Visual Communication and Image Representation*, vol. 82, p. 103401, 2022.

33) V. Kumar, V. Kansal, and M. Gaur, "Multiple forgery detection in video using convolution neural network," *Computers, Materials & Continua*, vol. 73, no. 1, 2022.

34) P. Priyanka, O. K. Rajesh, and M. Baburaj, "Matrix decomposition based digital video forgery detection," in *2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)*, pp. 403-406, 2022.

35) V. Kumar and M. Gaur, "Multiple forgery detection in video using inter-frame correlation distance with dual-threshold," *Multimedia Tools and Applications*, vol. 81, no. 30, pp. 43979-43998, 2022.

36) M. R. Oraibi and A. M. Radhi, "Enhancement digital forensic approach for inter-frame video forgery detection using a deep learning technique," *Iraqi Journal of Science*, pp. 2686-2701, 2022.

37) N. Girish and C. Nandini, "Inter-frame video forgery detection using UFS-MSRC algorithm and LSTM network," *International Journal of Modeling, Simulation, and Scientific Computing*, vol. 14, no. 01, p. 2341013, 2023.

38) N. A. Shelke and S. S. Kasana, "Multiple forgery detection in digital video with VGG-16-based deep neural network and KPCA," *Multimedia Tools and Applications*, vol. 83, no. 2, pp. 5415-5435, 2024.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13828734

39) H. Kaur and N. Jindal, "Deep convolutional neural network for graphics forgery detection in video," *Wireless Personal Communications*, vol. 112, pp. 1763-1781, 2020.

40) S. Dhivya and B. Sudhakar, "Copy move forgery detection using loopy RNN and SURF based high level moving object feature in video frame," 2020.

41) V. Vinolin and M. Sucharitha, "Dual adaptive deep convolutional neural network for video forgery detection in 3D lighting environment," *The Visual Computer*, vol. 37, pp. 2369-2390, 2021.

42) J. Bakas, R. Naskar, M. Nappi, and S. Bakshi, "Object-based forgery detection in surveillance video using capsule network," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-11, 2021.

43) Daniya, T., Aluri, S., Velliangiri, S., & Cristin, R. (2021, October). Copy-move forgery detection in videos using machine learning algorithm. In *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1502-1506). IEEE

44) Vinolin, V., & Sucharitha, M. (2021, December). Video forgery detection using distance-based features and deep convolutional neural network. In *2021 4th International Conference on Computing and Communications Technologies (ICCCT)* (pp. 350-355). IEEE.

45) Raskar, P. S., & Shah, S. K. (2021). Real time object-based video forgery detection using YOLO (V2). *Forensic Science International*, 327, 110979.

46) Tan, S., Chen, B., Zeng, J., Li, B., & Huang, J. (2022). Hybrid deep-learning framework for object-based forgery detection in video. *Signal Processing: Image Communication*, 105, 116695.

47) Ch, L. K., & PRASAD, K. (2022). Optimized deep learning model for spatio-temporal detection and localization of object removal video forgery with multiple feature extraction.

48) Raskar, P. S., & Shah, S. K. (2022). VFDHSOG: copy-move video forgery detection using histogram of second order gradients. *Wireless Personal Communications*, 122(2), 1617-1654.

49) Shelke, N. A., & Kasana, S. S. (2022). Multiple forgery detection and localization technique for digital video using PCT and NBAP. *Multimedia Tools and Applications*, 81(16), 22731-22759.

50) Zhao, C., Li, X., & Younes, R. (2023, March). Self-supervised Multi-Modal Video Forgery Attack Detection. In *2023 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1-6). IEEE.

51) Singla, N., Singh, J., & Nagpal, S. (2023). Raven finch optimized deep convolutional neural network model for intra-frame video forgery detection. *Concurrency and Computation: Practice and Experience*, 35(3), e7516.

52) Mohiuddin, S., Malakar, S., & Sarkar, R. (2023). An ensemble approach to detect copy-move forgery in videos. *Multimedia Tools and Applications*, 1-20.

53) Li, Q., Wang, R., & Xu, D. (2023). A Video Splicing Forgery Detection and Localization Algorithm Based on Sensor Pattern Noise. *Electronics*, 12(6), 1362.

54) H. D. Panchal, "Passive Video Forgery Detection," Ph.D. dissertation, Gujarat Technological University, Ahmedabad, India.